Le 10 septembre 2016

Lemme. *Soit $G$ un groupe fini. Il existe une extension de corps de nombres $K/k$, galoisienne de groupe $G$, qui est non ramifiée.*

Démonstration. Il sufft d'établir le résultat pour tout groupe symétrique $S_n$. Soit $k$ un corps de nombres. Soit $X = \mathrm{Spec}k[x_1, \ldots, x_n]$ et $Y = \mathrm{Spec}k[\sigma_1, \ldots, \sigma_n]$, où les $\sigma_i$ sont les fonctions symétriques des $x_j$. On dispose de l'application quotient $X \to Y$, qui est ramifiée mais génériquement galoisienne de groupe $S_n$. Comme $Y$ est un espace affine, on peut appliquer le théorème d'irréductiblité de Hilbert pour trouver des points $M \in k^n$ de fibre le spectre d'un corps. On peut faire plus. Soit $T$ un ensemble fini de places de $k$. Le théorème d'irréductibilité de Hilbert avec approximation faible (Ekedahl) permet de trouver un point de $k^n$ dont la fibre est le spectre d'un corps $K$ tel que pour tout $v \in T$ le produit tensoriel $K \otimes_k k_v$ est un produit de corps. On choisit pour $T$ l'ensemble des places archimédiennes et des places non archimédiennes de caractéristique résiduelle au plus $n$.

L'extension $K/k$ obtenue est donc galoisienne de groupe $S_n$ et déployée aux places $v \in T$, donc non ramfiée en ces places. Elle est donc modérément ramifiée. Soit $R$ l'ensemble des places de $k$ qui sont ramifiées dans $K$. Pour toute extension finie de corps $L/k$ linéairement disjointe de $K/k$ telle que $L = K \otimes_k L$ soit un corps, noté alors $KL$ l'extension $LK/L$ est une extension de corps modérément non ramifiée galoisienne de groupe $S_n$, ramifiée au plus en les places de l'ensemble $R_L$ des places de $L$ au-dessus de places de $R$. Soit $v$ une place finie de $k$ ramifiée dans $K$ et soit $\ell$ un premier divisant l'exposant de ramification. Par approximation faible dans $k$, on peut trouver $b \in k^*$ tel que $v(b) = 1$ et qu'il existe une valuation $w$ de $k$ non ramifiée dans $K$ avec $w(b) = 1$. L'extension $k_1 = k(b^{1/\ell})$ est alors linéairement disjointe de $K/k$. L'extension de corps $Kk_1/k_1$ est alors galoisienne de groupe $S_n$, ramifiée au plus au-dessus des places de $R_{k_1}$. D'après le lemme d'Abhyankhar, aux places de $k_1$ situées au-dessus de la place $v$, l'exposant de ramification a été divisé au moins par $\ell$. En continuant ce processus, on se débarrasse de toute la ramification.

Soit $G$ un groupe fini et $M$ un $G$-réseau. On note

$$Sha^2_{cycl}(G, M) := \mathrm{Ker}[H^2(G, M) \to \prod_{g \in G} H^2(< g >, M)].$$

Proposition. *Soit $G$ un groupe fini et $M$ un $G$-réseau. Si pour tout corps de nombres $k$ et tout $k$-tore de groupe des caractères $\hat{T}$ isomorphe au module galoisien $M$ on peut montrer $Sha^1(k, T) = 0$, alors :*

*(a) On a $Sha^2_{cycl}(G, M) = 0$.*

*(b) Sur tout corps de nombres $k$, tout $k$-tore de groupe des caractères $\hat{T} = M$ satisfait l'approximation faible.*

Démonstration. Par la dualité de Tate-Nakayama, pour tout corps de nombres $k$ et tout $k$-tore $T$ déployé par une extension finie galoisienne $K/k$ de groupe $G$ le groupe $Sha^1(k, T)$ est dual de $Sha^2(G, \hat{T})$, groupe défini par la nullité des restrictions aux sous-groupes de décompositions de $K/k$ . D'après le lemme il existe une extension non ramifiée $K/k$ de corps de nombres galoisienne de groupe $G$. Ses groupes de décomposition sont donc tous cycliques. Le théorème de Tchebotarev assure que tout sous-groupe cyclique est un groupe de décomposition. Pour une telle extension on a donc $Sha^2_{cycl}(G, M) = Sha^2(G, M)$, dual de $Sha^1(k, T)$, nul sous l'hypothèse de la proposition. Ceci établit (a).

Une fois (i) établi, pour obtenir (ii), on utilise la suite exacte de Voskresenskiĭ (Thm. 11.6 de [V]) et l'identification (Prop. 9.5 de [CTS2]) de son terme médian avec le dual de $Sha^2_{cycl}(G, M)$. Voir aussi la Prop. 19 p. 220 de [CTS1]). On peut d'ailleurs établir cette suite exacte en combinant résolutions flasques et Tate-Nakayama, sans introduire de compactification lisse de tore.

Application. Le cas des équations $c = Norm_{K/k}(x).Norm_{L/k}(y)$ avec $K/k$ extension cyclique de corps et $L/k$ extension quelconque de corps.

Ce cas particulier d'un résultat général du récent travail de Bayer, Lee, Parimala avait été obtenu par voie arithmétique (utilisation du théorème de Dirichlet sur les premiers dans une progression arithmétique, sur le corps de nombres $L$, et de la loi de réciprocité) avec J.-J. Sansuc en 1983. J.-J. Sansuc avait ensuite donné (en 1983) une démonstration purement algébrique de l'annulation de $Sha^2_{cycl}(G, \hat{T})$ pour le tore $T$ d'équation $1 = Norm_{K/k}(x).Norm_{L/k}(y)$, avec $K/k$ et $L/k$ comme ci-dessus. Le cas $L/k$ galoisien et linéairement disjoint de $K/k$ avait été traité par Hürlimann à la même époque.

Références :

[CTS1] J.-L. Colliot-Thélène et J.-J. Sansuc, La R-équivalence sur les tores, Ann. Sc. ENS, 4è série, **10** (1977) 175–229.

[CTS2] J.-L. Colliot-Thélène et J.-J. Sansuc, Principal homogeneous spaces under flasque tori : applications, J.Algebra **106** (1987) 148–205.

[E] T. Ekedahl, An effective version of Hilbert's irreducibility theorem. Séminaire de Théorie des Nombres, Paris 1988–1989, 241–249, Progr. Math. **91**, Birkhäuser Boston, Boston, MA, 1990.

[V] V. E. Voskresenskiĭ, Algebraic groups and their birational invariants, Transl. of Math. Monographs **179**, Amer. Math. Soc.